Information Security Policy.

The purpose of this policy is to describe the principles of information security defined by Temera, in order to develop an efficient and reliable Information Security Management System in accordance with ISO 27001:2022.

For Temera, the primary objective of Information Security is the protection of data and information, the technological, physical, logical and organizational structure, which is responsible for their management. This means obtaining and maintaining a reliable information management system, through compliance with the following properties:

1. **PRIVACY**: ensure the information is accessible only to those duly authorised;
2. **INTEGRITY**: safeguard the information consistency against unauthorised changes;
3. **AVAILABILITY**: ensure authorized users have access to information and associated architectural elements when they request it;
4. **MONITORING**: ensure data management is always carried out through reliable and tested processes and tools.

As part of the services management offered by Temera, through its technological infrastructure, it ensures:
- the guarantee of having a reliable partner for the treatment of its own informative patrimony;
- a great corporate image;
- the full compliance with Service Standards established with customers;
- customer satisfaction;
- compliance with current regulations and international safety standards.
- compliance with personal data protection regulation.

For this reason, Temera has developed a safe information management system following the requirements specified in ISO 27001:2022, and the mandatory laws as a means of managing information security within its business.

Temera's information security policy applies to all internal personnel and third parties (e.g.: service providers, maintenance, assistance, etc.) which collaborate on information management and all the processes and resources involved in the design, implementation, start-up and continuous services delivery.

Annually, Temera defines and revalidates the context in which it operates, the involved actors, opportunities and possible risks impacting on its Information Security Management System.

Temera's information security policy represents the organization's commitment to customers and third parties to ensure information security, physical, logical and organisational tools for data processing in any activities.

Temera's information security policy is based on the following principles:
a) to provide access control (see Annex "Access Control Policy");
b) to establish information classification (and processing) (see information classification);
c) to guarantee workplace physical and environmental safety;
d) to adopt end-user themes, such as:
- an acceptable use of assets;
- monitor and clean desk best-practices;
- appropriate transfer of information;
- regulated use of mobile devices and smart-working;
- limitations on installation and use of software;
e) regularly backup;
f) to establish safe information transfer procedures;
g) to provide malware protection;
h) to identify, monitor and manage technical vulnerabilities;
i) if needed, provide cryptographic controls;
j) to ensure the security of communications;
k) comply with current regulations in the field of privacy and protection of personal data;
l) to regulate the relations of suppliers in the light of ISO27001:2022.
m) Periodical verification of Temera information in public database and dark web.

This policy applies to the following field of application in reference to the activities carried out by Temera: **DESIGN, IMPLEMENTATION AND ASSISTANCE OF SOLUTIONS BASED ON INNOVATIVE IoT TECHNOLOGIES APPLICATIONS**.